UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/715,932	11/17/2003	Sunil K. Srivastava	50325-0854	4247

29989 7590 09/23/2004

HICKMAN PALERMO TRUONG & BECKER, LLP
1600 WILLOW STREET
SAN JOSE, CA 95125

EXAMINER	
LAFORGIA, CHRISTIAN A	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 09/23/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/715,932	SRIVASTAVA, SUNIL K.	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 May 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *5/10/04, 4/22/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-30 are presented for examination.

Priority

2. It is noted that this application appears to claim subject matter disclosed in prior Application No. 09/393,410, filed 10 September 1999. A reference to the prior application must be inserted as the first sentence of the specification of this application or in an application data sheet (37 CFR 1.76), if applicant intends to rely on the filing date of the prior application under 35 U.S.C. 119(e) or 120. See 37 CFR 1.78(a). For benefit claims under 35 U.S.C. 120, the reference must include the relationship (i.e., continuation, divisional, or continuation-in-part) of all nonprovisional applications. Also, the current status of all nonprovisional parent applications referenced should be included.

3. If the application is a utility or plant application filed under 35 U.S.C. 111(a) on or after November 29, 2000, the specific reference to the prior application must be submitted during the pendency of the application and within the later of four months from the actual filing date of the application or sixteen months from the filing date of the prior application. If the application is a utility or plant application which entered the national stage from an international application filed on or after November 29, 2000, after compliance with 35 U.S.C. 371, the specific reference must be submitted during the pendency of the application and within the later of four months from the date on which the national stage commenced under 35 U.S.C. 371(b) or (f) or sixteen months from the filing date of the prior application. See 37 CFR 1.78(a)(2)(ii) and (a)(5)(ii). This time period is not extendable and a failure to submit the reference required by 35 U.S.C. 119(e) and/or 120, where applicable, within this time period is considered a waiver of any

benefit of such prior application(s) under 35 U.S.C. 119(e), 120, 121 and 365(c). A priority claim filed after the required time period may be accepted if it is accompanied by a grantable petition to accept an unintentionally delayed claim for priority under 35 U.S.C. 119(e), 120, 121 and 365(c). The petition must be accompanied by (1) the reference required by 35 U.S.C. 120 or 119(e) and 37 CFR 1.78(a)(2) or (a)(5) to the prior application (unless previously submitted), (2) a surcharge under 37 CFR 1.17(t), and (3) a statement that the entire delay between the date the claim was due under 37 CFR 1.78(a)(2) or (a)(5) and the date the claim was filed was unintentional. The Director may require additional information where there is a question whether the delay was unintentional. The petition should be addressed to: Mail Stop Petition, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. The term "approximately" in claims 8, 10, 16, 18, 27, and 29 is a relative term which renders the claim indefinite. The term "approximately" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

6. Claims 12-19 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The variable “n” is undefined.

7. Claims 10, 12-19, and 29 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which

applicant regards as the invention. It has been held that the functional "whereby" statement does not define any structure and accordingly cannot serve to distinguish. See *In re Mason*, 114 USPQ 127, 44 CCPA 937 (1957).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1, 3, 11, 12, 19, 20, 22, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 4,200,770 to Hellman et al., hereinafter Hellman, in view of U.S. Patent No. 5,841,864 to Klayman et al., hereinafter Klayman.

10. As per claims 1, 12, and 20, Hellman discloses sending a first value associated with the first node to the second node, and receiving from the second node a second value associated with the second node, see column 2, lines 35-53;

generating a collective public key that is based upon the first private value and the second private value, see column 2, lines 42-53.

11. Hellman does not disclose where the values are private values and wherein the second value is obtained by using the intermediate shared secret key and communicating a collective public key that is based upon the first private value and the second private value to a third node of the network and receiving an individual public key from the third node and computing and storing the group shared secret key based upon the individual public key.

12. It would have been obvious to one of ordinary skill in the art at the time the invention was made to transmit the private values, since it is known to those of ordinary skill in the art that very few have access to the private values, if at all, in addition to them being more difficult to decipher. Private values are also known to generate the public key in public/private key pairs. Therefore, by using the combination of the two private values creates a more secure public cipher for the two nodes involved. For a better discussion of private keys to generate public keys please refer to pages 33-35 and Section 3.1 of **Applied Cryptography**, by Bruce Schneier.

13. It would have been obvious to one of ordinary skill in the art at the time the invention was made to repeat the Diffie-Hellman exchange with the public key generated by the first and second nodes with the public key of the third node, since it has been held that the mere duplication of a procedure requires only routine skill in the art. See MPEP 2144.04; see *In re Harza*, 274 F.2d 669, 671, 124 USPQ 378, 380 (CCPA 1960).

14. Hellman does not teach generating a session key.

15. Klayman discloses generating an intermediate shared secret key by issuing communications to a second node of the network, see Figure 1, block 402, and column 4, lines 61-67.

16. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a session key, since it is known to those of ordinary skill in the art that session keys reduce the risk of the data being compromised since session keys are only used once and then destroyed. For a better discussion of session keys please refer to pages 33-35 and Section 3.1 of **Applied Cryptography**, by Bruce Schneier.

17. Regarding claims 3 and 22, Hellman teaches wherein the public-key process is Diffie-Hellman key exchange.

18. Regarding claims 11, 19, and 30, Hellman teaches wherein generating the shared secret key value comprises computing and storing the shared secret key value "k"' at the first node according to the relation

$$k = C^{ab} \bmod (q) = p^{abc} \bmod (q)$$

wherein C, a, b, c, q, and p are values stored in a memory, and wherein C is the individual public key, a is the private value of the first node, b is the private value of the second node, c is a third private value of the third node, p is a base value, and q is a prime number value (column 4, lines 51-67; column 5, lines 11-39).

19. Claims 2, 4-7, 13-15, 21, and 23-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hellman in view of Klayman as applied to claim 1 above, and further in view of U.S. Patent No. 5,633,933 to Aziz, hereinafter Aziz.

20. Regarding claims 2, 13, and 21, Hellman and Klayman do not joining the first node to an initial multicast group in response to generating the intermediate shared secret key and joining a second node to a new multicast group that subsumes the initial multicast group after receiving the individual public key.

21. Aziz teaches joining the first node to an initial multicast group in response to generating the intermediate shared secret key (column 2, lines 45-53; column 8, line 30 to column 9, line 7); and

joining a second node to a new multicast group that subsumes the initial multicast group after receiving the individual public key (column 2, lines 45-53; column 8, line 30 to column 9, line 7). It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the multicast groups of Aziz in the combined system of Klayman and Hellman. One would be motivated to include the multicasting capabilities in the combined system of Klayman and Hellman, as it would be advantageous to provide a method to send an encrypted message to multiple users once instead of resending the same message multiple times.

22. Regarding claims 4, 14, and 23, Hellman and Klayman do not disclose wherein the step of communicating the collective public key further comprises determining whether the first node or the second node transfers the collective public key based upon an order of entry of such nodes into a multicast group.

23. Aziz teaches wherein the step of communicating the collective public key further comprises determining whether the first node or the second node transfers the collective public key based upon an order of entry of such nodes into a multicast group (column 2, lines 45-53; column 8, line 30 to column 9, line 7). It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the order of entry of Aziz in the combined system of Hellman and Klayman. One would be motivated to include the order of entry capabilities in the combined system of Hellman and Klayman, as it would be advantageous to provide a method to send an encrypted message to multiple users based on how long they have been a member of the multicast group.

24. Regarding claims 5 and 24, neither Hellman nor Klayman disclose wherein the step of communicating the collective public key further comprises determining whether the first node or the second node transfers the collective public key based upon a predetermined metric.

25. Aziz teaches wherein the step of communicating the collective public key further comprises determining whether the first node or the second node transfers the collective public key based upon a predetermined metric (column 2, lines 45-53; column 8, line 30 to column 9, line 7). It would have been obvious to one of ordinary skill in the art at the time the invention was made to send the key to the next node based upon a predetermined metric. One would be motivated to include the predetermined metric, as it would be advantageous to provide a method to send an encrypted message to multiple users based on the amount of time they have been associated with the multicast group.

26. Regarding claims 6 and 25, Hellman and Klayman fail to disclose wherein sending the first private value and receiving the second private value further comprises computing the first private value as a random integer and receiving a second random integer as the second private value.

27. Aziz teaches wherein sending the first private value and receiving the second private value further comprises computing the first private value as a random integer and receiving a second random integer as the second private value (column 2, lines 32-35). It would have been obvious to one of ordinary skill in the art at the time the invention was made to generate a random integer. One would be motivated to include the random integer as it provides for the

most secure system. If the integer is generated pseudo-randomly or from a user input, it makes the system much more vulnerable and open to being cracked.

28. Regarding claims 7, 15, and 26, neither Hellman nor Klayman disclose creating and storing information at the first node that associates the first node, the second node, and the third node as a multicast group communicating over a packet switched network.

29. Aziz teaches creating and storing information at the first node that associates the first node, the second node, and the third node as a multicast group communicating over a packet switched network (column 2, lines 45-53; column 8, line 30 to column 9, line 7). It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the multicast groups. One would be motivated to include the multicasting capabilities because it would provide a method to send an encrypted message to multiple users once instead of resending the same message multiple times.

30. Claims 8, 10, 16, 18, 27, and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hellman in view of Klayman as applied to claim 1 above, and further in view of **Handbook of Applied Cryptography**, by Alfred J. Menezes et al., hereinafter Menezes.

31. Regarding claims 8, 10, 16, 18, 27, and 29, neither Hellman nor Klayman disclose wherein the steps of generating, sending, communicating, and receiving further comprise communicating approximately $2n + 2(n-1)$ total messages.

32. Menezes teaches wherein the steps of generating, sending, communicating, and receiving further comprise communicating approximately $2n + 2(n-1)$ total messages, p. 519-520. It would

have been obvious to one of ordinary skill in the art at the time the invention was made to minimize the number of messages, since it is held by those of ordinary skill in the art that the more messages, the greater chance the messages are to be deciphered by an eavesdropper. For more information please refer to pages 33-35 and Section 3.1 of **Applied Cryptography**, by Bruce Schneier.

33. Claims 9, 17, and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hellman in view of Klayman as applied to claim 1 above, and further in view of U.S. Patent No. 6,363,154 to Peyravian et al., hereinafter Peyravian.

34. Regarding claims 9, 17, and 28, neither Hellman nor Klayman disclose wherein the step of communicating the collective public key comprises storing the collective public key and receiving the collective public key using a key distribution center.

35. Peyravian teaches wherein the step of communicating the collective public key comprises storing the collective public key and receiving the collective public key using a key distribution center. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a key distribution center, since Peyravian states at column 1, lines 48-55 that such a modification would allow group members to communicate securely.

Conclusion

36. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

37. The following patents are cited to further show the state of the art with respect to key distribution, such as:

United States Patent No. 6,636,968 to Rosner et al., which is cited to show multi-node encryption and key delivery.

United States Patent No. 6,226,383 to Jablon, which is cited to show cryptographic methods for remote authentication.

United States Patent No. 6,055,575 to Paulsen et al., which is cited to show virtual private network.

United States Patent No. 5,761,305 to Vanstone et al., which is cited to show key agreement and transport protocol with implicit signatures.

United States Patent No. 4,578,531 to Everheart et al., which is cited to show encryption system and key distribution method.

United States Patent No. 5,724,425 to Chang et al., which is cited to show enhancing software security and distributing software.

38. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (703) 305-7704. The examiner can normally be reached on Monday thru Thursday 7-5.

39. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

40. Information Regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christian LaForgia
Patent Examiner
Art Unit 2131

clf

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100